

Bots March In

PC Magazine 12/14/04

Last year we warned you that hackers were increasingly striving to take control of computers and, unbeknownst to their owners, turn them into "zombies" to propagate porn and spam, or to launch denial-of-service (DoS) attacks against Web sites or networks (see <http://go.pcmag.com/zombies>). Although PC Magazine readers may have listened, apparently many others didn't, because Symantec's Internet Security Threat Report for the first six months of 2004 stated that the number of bot worms—frequently used to create armies of "zombie" computers—was up 600 percent in the past six months, making bots the second most common attack threat in that period.

Bots are small scripts designed to perform automated functions; they are not inherently bad. They are often used for unattended system and user maintenance, and they are occasionally found on instant-messenger networks as robotic helpers for users.

Malicious bots, though, are essentially Trojan-horse programs that open up a victim's machine to remote access. They are capable of spreading through a number of methods, but the majority use IRC networks and network shares to propagate, and IRC channels to "call home" to their attackers. Bot worms have among the most variations of any kind of worm; these variations include Rbots, SDBots, Gaobots, spybots (no relation to the antispyware software), and half a dozen others.

A recent 30-day Symantec listing of viruses and worms included five spybots, five IRCBots, and three Gaobots, all of which spread via IRC channels. There were also two SDBots, which spread through network shares, and several Microsoft vulnerabilities, such as MS04-011.

Sophos antivirus tracks the Rbot extensively; there are over 840 variations in its virus library. The latest, W32/Rbot.KZ, uses weak passwords on network shares and on three Microsoft vulnerabilities (MS03-007, MS04-011, and MS04-012).

McAfee lists a number of bots. One, the W32/Gaobot.Worm.gen bot, was reported to have 1,350 variants as of May 2004. Gaobot exploits vulnerabilities on unpatched Microsoft systems and weak passwords on networks. Trojan or bot functionality varies between the different Gaobot varieties, but all use IRC to communicate with the attacker.

There is no concrete demographic information about the bot authors, but some versions, such as the SDBot.AB, hint at what type of people they might be: This bot attempts to steal product license keys for a wide range of computer games. SDBot.AB can also accomplish a number of remote tasks: perform a DoS attack against a target host, retrieve system information, connect to a URL, upload and download files, execute programs, log keystrokes, sniff network packets, conduct port scans against other computers, or steal the Windows Product ID.

Bots' ability to sniff network packets has network professionals worried, as hackers could use this to obtain secure information such as passwords and financial data. A keystroke logger may capture passwords and usernames, but a packet sniffer can watch for log-ons to target sites such as banks or stock sites.

The best way to prevent bot infection is to keep Windows and your antivirus protection up to date. If you're on a network, using strong passwords will help prevent propagation through network shares. Disable any unused shares and services such as FTP. Use a firewall that monitors both incoming and outgoing activity, particularly one that is aware of applications usage of the Web, if you use IRC, and one that can block IRC ports (6667 is the most common) if you don't. A stateful packet inspection (SPI)-based firewall is the best. Both of our Editors' Choices, Norton Personal Firewall and ZoneAlarm Pro, are among the products that fill the bill.